Securing Your Wireless Network

Wireless networks are becoming increasingly popular, but they introduce additional security risks. If you have a wireless network, make sure to take appropriate precautions to protect your information.

Because wireless networks do not require a wire to connect between your computer and the Internet, it is possible for attackers to intercept an unprotected connection. A practice known as wardriving involves individuals, with a computer, a wireless card and a GPS device, driving through areas in search of wireless networks and identifying the coordinates of a network location. Individuals participating in wardriving have malicious intent and use the information to hijack your home wireless network or intercept the connection between your computer and a particular hotspot. What can you do to minimize the risks to your wireless network?

* **Change default passwords** - to simplify setup, most network devices, including wireless access points, are pre-configured with default administrator passwords so they don't provide protection. Changing default passwords makes it harder for attackers to take control of your device.
* **Restrict access** - only allow authorized users to access your network. Each piece of hardware connected to a network has a MAC (media access control) address. You can restrict or allow access to your network by filtering MAC addresses. Consult your user documentation to get specific information about enabling these features.
* **Encrypt data on your network** - WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) both encrypt information on wireless devices. However, WEP has a number of security issues that make it less effective than WPA, so you should specifically look for gear that supports encryption via WPA. Encrypting the data would prevent anyone who might be able to access your network from viewing your data.
* **Install a firewall** - While it is a good security practice to install a firewall on your network, you should also install a firewall directly on your wireless devices. Attackers who can directly tap into your wireless network may be able to circumvent your network firewall.
* **Maintain anti-virus software** - you can reduce the damage attackers can inflict on your network and wireless computer by installing anti-virus software and keeping your virus definitions up to date.

ADOA Information Security

AIS Managing Our Information Safeguards

For more information contact:
ADOA Information Security (AIS)
Visit Our Web Site: http://www.azdoa.gov/isd/ais
E-mail: AIS_SC@azdoa.gov
Phone: 602•542•2252

March 2008

Sun	Mon	Tue	Wed	Thu	Fri	Sat
						1
2	3	4	5	6	7	8
9	10	11	12	13	14 Pay Day	15
16	17 St. Patrick's Day	18	19	20 Spring	21	22
23 Happy Easter	24	25	26	27	28 Pay Day	29
30	31					